## REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Objection to Claims 3 and 11

This objection has been addressed by amending claims 3 and 11 to refer to *generation* of the disguised input data and operation by means of respective XOR operations.

2. Rejection of Claims 1-18 Under 35 USC §102(e) in view of U.S. Patent Publication No. 2001/0053220 (Kocher)

This rejection is respectfully traversed on the grounds that the Kocher publication does not disclose or suggest a data carrier having a semiconductor chip with a memory and operating program that disguises an operation h and its input x in order to obtain a disguised operation $h_{R1}$ and disguised input data $(x \otimes R_1)$, *i.e.*, in which:

$$h_{R1}(x \otimes R_1) = y = h(x)$$

holds true, with $h_{R1}$ being obtained by $h_{R1}(x)=h(x)\otimes R_1$.

**Instead of performing a disguised operation on disguised input data, Kocher only teaches disguising of the input data.** The operation performed on the disguised input data, which results from splitting the original data, is the same DES operation as would have been performed on the original data, albeit performed in two parallel operations on the respective parts of the input data split parts of the original key. Kocher does not teach disguising of the DES operation in the manner claimed, but only the input data and the DES keys. Furthermore, the disguised input of Kocher is not obtained by combining the input data with a random number using an exclusive OR operation. Thus, the method of Kocher lacks to features of the claimed invention.

The method described in the Kocher publication involves enhancing DES encryption by splitting a message M and a key K into permutated message components PM1 and PM2, and permutated key components PK1 and PK2, respectively, such that PM1 $\otimes$ PM2 = M and PK1 $\otimes$ PK2 = K holds (see paragraph [0035] of the Kocher publication). Thereafter, the two message/key pairs (PM1,PK1) and (PM2,PK2) are DES-encrypted separately instead of the standard pair (M,K), so that the resulting ciphertexts can be recombined to obtain the same ciphertext that is obtained when encrypting the original message M with the original K (as explained in paragraph [0036] of the Kocher publication. Thus, it holds that:

$$DES(PM1,PK1) \diamond DES(PM2,PK2) = DES(M,K)$$

where $\diamond$ symbolizes the recombination operation. The Examiner will note that there is no attempt to perform a disguised operation on the input in order to obtain the same output values that would be obtained if the original operation were performed on the original data, but only a splitting of data and keys, which has the effect of disguising the original data.

The essence of Kocher's teaching is to enhance security of DES by

- splitting each input parameter into two components,
- processing the components separately, and
- combining the results of the separate procedures.

This is fundamentally different than the claimed invention.

If a person of ordinary skill in the art were to apply Kocher's teachings to the problem of securing operation h(x), *i.e.*, if the claimed h(x) were considered to correspond to the DES algorithm used by Kocher, then the input x of h(x) would have to correspond to Kocher's message M and/or key K. However, in that case the person of ordinary skill in the art would be taught by Kocher to split the input (x) into a random component (R1) and a derived component (R2 = x $\otimes$ R1). The ordinary artisan would then, according to the teachings of Kocher, process

the two components by separately performing h(R1) and h(x⊗ R1), and finally recombine the results of the separate processing to obtain:

$$\mathbf{h(R1) \diamond h(x \otimes R1) = h(x).}$$

The Examiner will note that this result of applying the teachings of Kocher to an input x and operation h is not the same as the result of applying the claimed invention. The result of applying the teachings of Kocher to input data x and operation h is, h(R1) ◇ h(x ⊗ R1) = h(x), which is not equivalent to the claimed disguising operation $h_{R1}(x)=h(x)\otimes R_1$. Instead, Kocher performs the SAME operation h on the two components of original input data x, namely random number R1 and the combination of input data x and random number R1, and makes not attempt to disguise h.

Because the Kocher publication does not disclose or suggest disguising **both** input data and an operation performed on the input data, such that performing the disguised operation on the disguised input data yields the same result as performing the original operation on the original input data, it is respectfully submitted that the Kocher publication does not anticipate or suggest the claimed invention, and withdrawal of the rejection of claims 1-18 under 35 USC §102(e) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: April 7, 2005

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500